Quantum Computing: A Survey

Matt Defenthaler
School of Computer Science and Engineering
University of Central Florida
Orlando, FL 32826
mattanonymous@gmail.com

Abstract

After the concept came to fruition in the early 1980's quantum computing has enjoyed revolutionary advancements in the theory that deals with the manipulation of quantum particles and their measurement. The entire field of quantum computation is still in its early infancy despite these advancements. Only a handful of applicable algorithms exist and many have only been shown to be theoretically possible. There exists a great disconnect between quantum computational theory and real-world hardware capable of performing the operations required to execute algorithms in ways that make quantum computation a clear successor to its classical counterpart. The introduction of quantum computational theories, algorithms, hardware, and other necessary building blocks of quantum computing systems will create paths that are less than visible due to the current overall need for a better understanding of quantum mechanical interactions. The future of quantum computing exists in a superposition between states of uncertainty and optimism.

1 Introduction

While attempting to simulate quantum mechanical effects on a classical computer and realizing the shortcomings of doing so, Richard Feynman devised a concept that would utilize the properties of quantum mechanics to perform computations much faster than is possible with classical information processing technologies. In an effort to solve the impending problems that will come as a result of continuing to reduce the physical scale of computer processor circuitry, many physicists, engineers, and computer scientists began seriously considering this concept. Shortly after its introduction, it was met with much skepticism due to the problems presented by the lack of understanding the scientific community has of particle interactions on the quantum scale that would, in effect, make quantum computation seemingly impossible. In the 1990's however, quantum computation algorithms were theorized and appeared to be capable of exploiting quantum mechanical phenomena while also obeying the rules that govern quantum interactions. The algorithms provided motivation for the building of quantum computing hardware in order to realize the actual potential of the algorithms.

Quantum computing hardware operates by manipulating binary data stored in quantum particles. This can be compared to bits used by today's classical computers. However, an immense difference exists between quantum bits, qubits, and classical bits. This difference is in the quantum phenomenon known as superposition. Superposition allows a single qubit to represent two binary states, 0 and 1, simultaneously rather than just one of the states, 0 or 1. As a result, a manipulation to one qubit would be analogous to two classical bits. At first glance, this does not appear to be a significant improvement. Upon further observation, it can be realized that a greater number of qubits are capable of representing all of the $2^n$ classically possible values simultaneously. This reduces algorithm complexity by allowing calculations normally performed in many iterations to be performed in just a single iteration.

As with all phenomena, difficulties exist in attempts of exploitation. The mere properties that
allow for a potentially massive number of computation to be performed in parallel have their own unique rules that tend to counteract any form of manipulation.

2 Quantum Phenomenon

Classical physics describes the interactions between almost every grouping of particles large enough to be observed without special equipment. It fails, however, to describe the interactions that occur among subatomic particles. These interactions, when using classical physics as a frame of reference, are highly non-intuitive. Despite this and the fact that the field is still emerging, some of the interactions are understood well enough to exploit their properties. These properties are fundamental to the contrast between quantum and classical computers.

The most important aspects of quantum computing are the phenomena that exist in quantum mechanics. There is a significant difference in the way in which it is believed quantum particles interact and the way all other particles interact despite the fact that anything greater than an atom in size is composed of quantum particles. One of these aspects is quantum entanglement. "Entanglement is the potential of quantum states to exhibit correlations that cannot be accounted for classically."[1] An example of quantum entanglement can be observed when a photon is split and the resulting two photons are correlated in such a way that a change to one triggers a change in the other. This effect is independent of distance and has been the cause of great confusion since its discovery. It is important to note that quantum mechanics requires an interpretation. This comes as a result of a lack of understanding as to the causality of the interactions of quantum particles. An understanding of how something works is not necessarily required in order to utilize the resulting effects. Another important concept that gives quantum computation its great capacity for quickly performing operations is that of superposition. Superposition is most easily understood in its application to waves and wave functions. Two waves can combine to produce another wave, a child, that contains information about the two parent waves. Information about one parent can be deduced as long as information about the other parent waves is available. Another strange phenomena that exists in quantum mechanics is the apparent effect that measurement, or observation, has on quantum particles. Any attempt to measure the state, such as the position or momentum, of a quantum particle results in a change in the number of possible states of the particle. More specifically, the act of measuring a property of a quantum particle causes the superposition, or combination of all possible configurations, to collapse into a single, observable configuration. This is yet another topic that continues to be debated and is currently open for interpretation as to why and how this occurs.

3 Utilizing Quantum Phenomena

The parallelization that gives quantum computation its great potential is merely an exploitation of the principle of superposition. Superposition allows a particular computation to be applied to every discrete number in a finite set simultaneously[2]. The superposition is used as though it represents a single, finite number during quantum computation and, thus, computes all possibilities in parallel. There are various methods for extracting relevant data from the set composed of the computed data. One of these methods deals with having separated related values into two registers of entangled qubits and observing one of the registers to cause a partial collapse in the other register so that it only contains superpositions of numbers corresponding to the period observed in the other register. Another advantage of entanglement is the ability to perform error correction. Peter Shor developed a scheme for correcting errors in qubits caused by acts such as decoherence that used multiple entangled qubits. This was necessary as quantum computers can't use the classical error correction scheme, one that requires observation of the values prior to computation to create extra copies of the bits, due to the no-cloning theorem[lufeng].

4 Quantum Algorithms

Algorithms suitable for quantum computation are required to be probabilistic due to the lack of causality apparent in the states of quantum particles. The algorithms must also be capable of having their data processed in parallel. For instance, an algorithm composed of functions that use the output of one function as the input of another can-
not be parallelized as running the functions in any order other than that specified by the flow of the logic would result in unpredictable and useless data. This greatly restricts the number of problems that a quantum computer will be able to solve more quickly than a classical computer. As a result, the potential of quantum computers failed to be recognized until example algorithms were created that, in theory, allowed for a great improvement in runtime. The two most popular algorithms demonstrating the potential of quantum computation algorithms are Peter Shor's integer factorization algorithm and Lov Grover's search algorithm.

Peter Shor's integer factorization algorithm, more commonly known as simply "Shor's algorithm", was discovered by Shor in 1994 and has been shown to be capable of factoring an integer into its prime components. The main objective of the algorithm is to find the period of a periodic function, a function whose output values repeat over a given interval. The quantum part of the algorithm uses two quantum registers containing entangled qubits. Measuring one of the registers causes a projection corresponding to the observed measurement on to the other register. Next, the quantum fourier transform is used. The quantum fourier transform is a form of the discrete fourier transform that can be realized on a quantum computer through the use of Hadamard and phase shift gates. [lec13]The quantum fourier transform is applied to the register receiving the projection in order to peak the probability of measuring an exponential variable used in a classical algorithm to find a prime factor. Once one prime factor is found, a classical computer can quickly discover the other. This result produced by this algorithm can easily be verified on a classical computer through simple multiplication. If the result is wrong, as is possible due to the probabilistic nature of the system and the algorithm, the algorithm is run repeatedly until the correct answer is found. Since the time is so greatly reduced, multiple executions can be performed and a correct result can still be obtained in much less time than would be needed for a classical computer to accomplish the same task. More specifically, the best classical prime factorization algorithm has a time complexity of $O(e^{\sqrt{\ln(n)\ln(\ln(n))}})$, whereas using Shor's algorithm, the same can be accomplished in just $O(\ln(n))$.[2]

5 Quantum Computing Hardware

Without hardware to implement the theories that have been proposed for quantum computation, quantum computers amount to little more than science fiction. John Preskill[2] lists the requirements for physically implementing a quantum computation system as:

- **Storage**: Qubits will have to be stored long enough for useful calculations to be performed.
- **Isolation**: The qubits must be sufficiently isolated from the environment to avoid decoherence.
- **Readout**: Preparation and measurement of qubits should be efficient and reliable.
- **Gates**: A universal set of logical operations (gates) should be available for the manipulation of qubits.
- **Precision**: All operations should be implemented with high precision to ensure reliability.

5.1 Ion Traps

Ion traps are an invention of Wolfgang Paul and Hans Dehmelt in order to confine charged particles to a three dimensional space via an oscillating electric field and are one example of a method for developing a physical system for quantum computation. The electric field oscillates within the radio frequency of the electromagnetic spectrum to form a potential in the shape of a spinning saddle. Over time, the ions interacting with the oscillating potential become trapped in the center of the saddle. In 1995, Ignacio Cirac and Peter Zoller proposed a controlled-NOT quantum gate scheme for operating on data stored in quantum particles. The gate operates on the states of ions which are described as being in a superposition of the ground state and the excited state, which assume the values of 0 and 1 respectively[2].

The state of an ion in this system is initialized and observed by projecting the beam of a laser operating at specific energies. A selected qubit can be given the value of 1 by shining a specific frequency of laser light onto the ion until it assumes its excited state. Over time, the state of the ion will decay to the ground state. Observing the current state of an ion is performed in much the same way. If the ion is in the ground state, increasing its
energy through laser pulses will cause photons to be emitted as the state quickly decays. Ions in their excited state will not be affected by the laser's energy because it will be too small to further excite the ion. The lack of photon emission signifies a 1.

5.2 NMR

Nuclear Magnetic Resonance (NMR) is a fairly recent method used in quantum computing hardware. It makes use of the nuclear spins within a molecule to act as qubits. The spins are encoded by applying pulses of magnetic energy to the molecule. The frequency of these pulses are capable of targeting specific spins in much the same way as the frequency of the laser is capable of targeting specific ions in ion traps. Another somewhat unique characteristic of the system is that it encodes data in an ensemble of spins whereas most other systems deal with encoding information in a single property of a single particle. Ensemble encoding is used because of the relatively small amount of energy contained within a discrete spin. One of the benefits to using Nuclear Magnetic Resonance over other methods is the greater amount of time before information in the spins is lost to decoherence. There is currently some debate over whether or not NMR is actually feasible for quantum computation. There is concern over the scalability of the system and it is common opinion that the current implementation is not scalable. Even more important, there is debate over whether or not the NMR systems proposed should even be classified as quantum computing systems. This is due to the fact that NMR states can be described in a classical manner.[torino].

6 Limitations of Quantum Computation

6.1 Decoherence

The limits of quantum computation are directly responsible for the lack of quantum computers operating with a large number of qubits as well as the lack of practical applications introduced thus far. The greatest challenge is due to the issue of decoherence. Decoherence is the loss of information about the properties of a qubit describing its state. Considering the fact that mere measurement has an effect on these properties, it is easy to imagine how volatile the state information of a qubit is. In most cases, an attempt to resolve the problem of possible decoherence comes in the form of building an isolated system that cannot be affected by the outside environment.

6.2 Quantum Algorithm Design

Another area of difficulty in making quantum computing practical is in the designing of algorithms that benefit from parallel computation under the constraints of quantum mechanics. It is required that the algorithms be stochastic rather than deterministic. A quantum algorithm must cleverly utilize the fact that computational outcomes occur with certain probabilities. This provides difficulty over classical algorithms which deterministically come to a conclusion and one need not worry about incorporating mathematical and physical techniques to 'peak' the probabilities of results likely to be correct.

7 Future of Quantum Computing

Quantum computing is barely in its infancy. As more research is done and a greater number of minds are available to theorize what can be accomplished through quantum computation, the field will continue to grow and advance. The most important aspect in which the field can advance is in the building of hardware that can operate on and interact with many qubits. It was hypothesized by John Preskill that a quantum computer with 10^6 qubits have a probability of error that is less than 10^-6 are needed in order to exceed what is possible with classical prime factorization algorithms being executed on classical computers[apres]. Preskill also notes that, although achieving this will take great ambition, it is within the scope of what should be possible.

7.1 Decryption

Some areas of computer science take advantage of the current computational difficulties that exist in classical computing. One of these areas is cryptography which, in some cases, utilizes one-way functions, functions whose inverse is very difficult to compute, in order to provide a secure means of communication. These one-way functions often rely on the difficulty inherent in factoring a large
composite number into its large prime components. Peter Shor’s factorization algorithm, if implemented on sufficient hardware, would make public key encryption schemes, such as RSA, insecure due to the fact that they rely on the current difficulty of factoring a number into its primes for their security.

7.2 Scalability

Another determining factor of the future of quantum computing lies in scalability. All hardware built thus far has been purpose-built. In other words, the hardware was designed to run a single algorithm on a single quantum circuit. These circuits have dealt with only several qubits in order to avoid complications involved in systems responsible of manipulating large numbers of quantum particles. For any true potential to be realized, quantum computation systems must become more dynamic; not only in hardware, but also in programming and algorithm design. A number of designs have been proposed to extend existing quantum systems into the realm of practical size. In reality, with the rapid introduction of new, better techniques for manipulating quantum particles the future will bring vastly different systems for performing quantum computation that are difficult for most to foresee today[apres].

8 Conclusion

The concept of a computer that utilized the properties of quantum mechanics that was developed by Richard Feynman is only several decades old and, despite great progress, is only barely making the transition from theory to reality. The contributions of people like Peter Shor and David Deutsch have helped propel the momentum of the theory of quantum computing and its supporting feasibility forward. More specifically, this propulsion has been the result of the discovery of quantum computing algorithms, quantum error correction, theoretical physics on the quantum level, and hardware designs that have helped prove, although only on a basic level, that quantum computation is venerable. As researchers continue to experiment with and learn about the smallest quantifiable particles that science is aware of, more will become known about them and how they interact with each other and their environment. This information will prove to be of great use to those applying quantum mechanical properties to performing computation. There is a great potential associated with the great magnitude of parallelization possible in quantum systems and the potential continues to be realized as solutions are found to the problems that appear to be major roadblocks upon first glance. The fact still remains, however, that quantum computation can only provide an increase in processing capabilities for a specific set of computational problems.

References